

## ABSTRACT

A Chip Authentication Program based on 3-D Secure protocols is provided for authenticating customers' on-line transactions. An issuer, who may be a payment card issuer, operates Access Control and Authentication Request Servers for authenticating transactions by individual customers who are identified by their personal EMV-complaint smart cards. An authentication token is generated at the point of interaction (POI) for each transaction based on information from the customer's smart card and transaction specific information sent directly by the issuer to populate a web page at the POI. Authentication tokens generated at the POI are evaluated by the Authentication Request Server to authenticate individual customer and/or card presence at the transaction POI. Authentication values are transported on-line in designated Universal Cardholder Authentication Fields consistent with 3-D Secure protocols.